REMARKS

Reconsideration and allowance of the present application are respectfully requested. Claims 1-44 and 48-51 remain pending in the application. By this Amendment, claims 1-3, 5-7, 13, 24, 35, 48 and 49 are amended. No new matter is added.

In numbered paragraph 6, pages 2-17 of the final Office Action, claims 1-18, 24-29, 35-41 and 48-51 have been rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Patent No. 5,872,917 to (Hellman) in view of U.S. 2005/0138355 (Chen et al.). In numbered paragraph 7, pages 18-20 of the final Office Action, claims 19-23, 30-34 and 41-44 have been rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over the Hellman patent in view of the Chen et al. patent, and further in view of U.S. Patent No. 7,155,607 (Yokota et al.). These rejections are respectfully traversed.

Applicants have discussed of record Applicants' disclosure of an exemplary server computer 14 which generates a credential (cred) for a client computer 12 in step 310 that proves the identity of the client computer 12. For the embodiment shown in FIG. 3, Applicants have disclosed that in step 304, an exemplary server computer chooses security parameters and an expiration time (exp) for the credential. In the illustrated embodiment, the security parameters include a hash seed (s), and a maximum number of times (m) to run a hash function (e.g., specification at paragraph [0024]). Applicants have further discussed of record that in step 312, a server computer 14 transmits the session information (sessioninfo), seed (s), maximum times (m) to run the hash function, the expiration time (exp), and

the credential (cred) encrypted by the initial session key (k1) to the client computer 12 in order to issue the credential. (e.g., specification at paragraph [0025]).

The foregoing features are broadly encompassed by claim 1, which recites a method for authenticating a computing device, including among other features, issuing a credential based on session information, a hash seed, a maximum iterative value, credential information and an expiration time from a first computing device to a second computing device, transmitting said credential and a computer challenge from the second computing device to the first computing device when the second computing device is to be authenticated, transmitting a response to said computer challenge from said first computing device to said second computing device, and verifying said response with said second computing device in order to authenticate and verify said computing devices.

Hellman illustrates in FIG. 1 a data flow between user and host computers 10 and 12, respectively. The Examiner has admitted on page 3 of the Office Action that "Hellman does not explicitly disclose issuing a credential based on session information, security parameters, credential information and an expiration time from a first computer to a second computer and authentication of the computers." At least for these reasons, the Hellman patent would not have taught the features of claim 1, including the recited features of issuing a credential based on session information, a hash seed, a maximum iterative value, credential information and an expiration time from a first computing device to a second computing device, ...and verifying said response with said second computing device in order to authenticate and verify said computing devices. Claims 7, 13, 24, 35, 48 and 49 similarly recite at least the features of issuing a credential based on session information, a hash seed, a

maximum iterative value, credential information and an expiration time from a first computer to a second computer.

The Chen et al. publication does not cure the deficiencies of the Hellman patent. The Chen et al. publication was applied for its various disclosures relating to a system for authentication in a wireless local area network (WLAN) including a CDMA2000 authentication center for authenticating CDMA2000 credentials (e.g., paragraph [0016]). But this and other related Chen et al. disclosures are based on wireless mobile communications, e.g., cell phones. The wireless mobile communications as disclosed in the Chen et al. publication are not on point as to the Applicants' claimed features relating to issuing a credential specifically from a first computing device to a second computing device.

For example, nowhere in the Chen et al. publication can one find any mention of session information, a hash seed, a maximum iterative value, credential information and an expiration time forming a basis for issuing a credential. Rather, while the Examiner appears to have erroneously relied on a mention of a CDMA 2000 global challenge and response (paragraph [0024]); and a brief mention of a shared secret data (SSD) (paragraph [0025]), they relate to wireless broadcasts involving an over-the-air mobile phone technology. These and other disclosures that the Examiner relies on would not have taught or suggested specifically, among other recited features, issuing a credential based on session information, a hash seed, a maximum iterative value, credential information and an expiration time from a first computing device to a second computing device, ...and verifying said response with said second computing device in order to authenticate and verify said

computing devices, as recited in claim 1, and as similarly recited in claims 7, 13, 24, 35, 48 and 49.

The Yokota et al. patent does not cure the deficiencies of the Hellman patent and the Chen et al. publication. The Yokota et al. patent was applied by the Examiner for the disclosure of a random number generating unit operating with a challenge data sending unit for the purpose of "judging whether or not to authenticate the second apparatus by determining if the piece of response data and the random number are identical" (col. 5, line 65 through col. 6, line 15). However, the Yokota et al. patent, even if combined with the Hellman patent and the Chen et al. publication as the Examiner has suggested, would not have taught or suggested issuing a credential based on session information, a hash seed, a maximum iterative value, credential information and an expiration time from a first computing device to a second computing device, ...and verifying said response with said second computing device in order to authenticate and verify said computing devices, as recited in claim 1, and as similarly recited in claims 7, 13, 24, 35, 48 and 49.

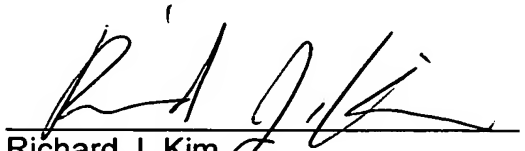
For at least these reasons, Applicants' claims 1, 7, 13, 24, 35, 48 and 49 are allowable. The remaining claims depend from the respective independent claim, and recite additional advantageous features which further distinguish over the documents relied upon by the Examiner. As such, the present application is in condition for allowance.

All objections and rejections raised in the Office Action having been addressed, it is respectfully submitted that the application is in condition for allowance and a Notice of Allowance is respectfully solicited.

In the event that there are any questions concerning this paper, or the application in general, the Examiner is respectfully urged to telephone Applicants' undersigned representative so that prosecution of the application may be expedited.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: September 12, 2008 By: 

Richard J. Kim
Registration No. 48360

P.O. Box 1404
Alexandria, VA 22313-1404
703 836 6620